



[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

NTRU key encapsulation

1950

- 2001

Search

Ad
Sc
Sc

☒ Search only in Engineering, Computer Science, and Mathematics.

☐ Search in all subject areas.

Your search - NTRU key encapsulation - did not match any articles published between 1950 and 2001.

Suggestions:

- Make sure all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.
- Try searching in all subject areas.
- Try searching over a larger date range.
- Try your query on the entire web.

[Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2008 Google



[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

NTRU shared-key distribution

1950

- 2002

Search

Ad
Sc
Sc

☒ Search only in Engineering, Computer Science, and Mathematics.

☐ Search in all subject areas.

Scholar

Results 1 - 2 of 2 for NTRU shared-key distribution. (0.28 seconds)

All Results

[CITATION] [Non-malleable cryptography - all 19 versions »](#)

[D Dolev](#)

D Dolev, C Dwork, M Naor - Computing, 2000

[C Dwork](#)

... to achieve than NM-CCA- post), combined with any shared-key cryptosystem that ... and Jaulmes and Joux [74] exploited these issues in attacking variants of NTRU. ...

[M Naor](#)

[Cited by 654](#) - [Related Articles](#) - [Web Search](#) - [Library Search](#)

[PDF] [Perspectives](#)

IW LAN - Computing, 2001 - cnp-wireless.com

... authenticated by the distribution system (see Figure 1 ... same response based on the shared key, validation is ... Jeffrey Hoffstein Assignee: NTRU Cryptosystems, Inc. ...

[View as HTML](#) - [Web Search](#)

NTRU shared-key distribution

Search

[Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2008 Google

- ☒ Search only in Engineering, Computer Science, and Mathematics.
☐ Search in all subject areas.

Scholar All articles - [Recent articles](#) Results 1 - 10 of about 13 for public key "key encapsulation"

All Results

[V Shoup](#)

[J Nieto](#)

[K Viswanathan](#)

[C Boyd](#)

[E Dawson](#)

[PDF] [A proposal for an ISO standard for public key encryption \(version 2.1\) - all 11 versions »](#)

V Shoup - Manuscript, 2001 - [mirror.cr.yp.to](#)

... This "proof" was published in [BR94], and despite years of public scrutiny, it was ... that use RSA-OAEP use it simply as a key encapsulation mechanism, which ...

[Cited by 94](#) - [Related Articles](#) - [View as HTML](#) - [Web Search](#)

[Using Hash Functions as a Hedge against Chosen Ciphertext Attack - all 13 versions »](#)

V Shoup - [Advances in Cryptology-Eurocrypt 2000, 2000](#) - [books.google.com](#)

... A key encapsulation scheme works just like a public key encryption scheme, except that the encryption algorithm takes no input other than the recipient's ...

[Cited by 82](#) - [Related Articles](#) - [Web Search](#) - [Library Search](#)

[Key Recovery System for the Commercial Environment - all 4 versions »](#)

JG Nieto, K Viswanathan, C Boyd, E Dawson - [Information Security and Privacy: 5th Australasian ...](#), 2000 - [books.google.com](#)

... a session key encrypted under the KRA's public key. ... KR techniques are commonly categorised into two types: key escrow and key encapsulation [17]. ...

[Cited by 7](#) - [Related Articles](#) - [Web Search](#)

[PS] [A Proposal for an ISO Standard for Public Key Encryption \(Version 1.1\) - all 2 versions »](#)

V Shoup - [ISO/IEC JTC 1/SC, 2001](#) - [shoup.net](#)

... 4.2 Preliminaries 8.2.1 Public-key encryption and chosen ciphertext attack 8.2.2 Key encapsulation

[Cited by 3](#) - [Related Articles](#) - [View as HTML](#) - [Web Search](#)

[Specification and analysis of n-way key recovery system by Extended Cryptographic Timed Petri Net - all 4 versions »](#)

SY Lim, JH Ko, EA Jun, GS Lee - [The Journal of Systems & Software](#), 2001 - Elsevier

... 4. Key encapsulation (eg, RecoveryKey (Walker et al., 1996), CyKey ... session-key, then

asymmetrically encrypts the session-key using the public-key of Key ...

[Cited by 4](#) - [Related Articles](#) - [Web Search](#)

[Remarks on KRA key recovery block format - all 2 versions »](#)

K Rantos, C Mitchell - [Electronics Letters](#), 1999 - [ieeexplore.ieee.org](#)

... If the receiver does not have a public key because he is not using key escrow but a key encapsulation mechanism (or a public key that he might have does not ...

[Cited by 3](#) - [Related Articles](#) - [Web Search](#)

[Key Recovery Scheme Interoperability-AProtocol for Mechanism Negotiation - all 7 versions »](#)

K Rantos, CJ Mitchell - Cryptography and Coding: 8th IMA International Conference, ..., 2001 - [books.google.com](#)

... key encapsulation schemes appear to be more adaptable in this respect, since they simply wrap the generated data encryption key under the KRA's public ...

[Cited by 2](#) - [Related Articles](#) - [Web Search](#)

Why use Digital Signatures for Electronic Commerce?' - all 8 versions »

J Angei - Commentary, 1999 - [www2-test.warwick.ac.uk](#)

... will be the driving force behind the development of many new services which vary from certification (eg likely to identify with a public key) to fully fledged ...

[Cited by 5](#) - [Related Articles](#) - [Cached](#) - [Web Search](#)

Design of key recovery system using multiple agent technology forelectronic commerce

SY Lim, HS Hani, MJ Kim, TY Kim - Industrial Electronics, 2001. Proceedings. ISIE 2001. IEEE ..., 2001 - [ieeexplore.ieee.org](#)

... 4. Key encapsulation (eg, RecoveryKey[23], CyKey [18], SecretAgent[2], IBM ... key, then

asymmetrically encrypts the session-key using the public- key of Key ...


[Web Search](#)

Security techniques for the global information infrastructure

W Fumy, I Haas - Global Telecommunications Conference, 1998. GLOBECOM 98. The ..., 1998 - [ieeexplore.ieee.org](#)

... is the development of certification services and of a public-key infrastructure to ... Key recovery, key escrow and key encapsulation are techniques that can help ...

[Related Articles](#) - [Web Search](#)

Google 

Result Page: 1 [2](#) [Next](#)

[Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2008 Google



[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

shared key distribution PSEC KEM

1950

- 2002

Search

Ad
Sc
Sc

☒ Search only in Engineering, Computer Science, and Mathematics.

☐ Search in all subject areas.

Scholar

Results 1 - 2 of 2 for [shared key distribution PSEC KEM](#). (0.06 seconds)

All Results

[V Shoup](#)

[PDF] [A proposal for an ISO standard for public key encryption \(version 2.1\)](#) - [all 11 versions »](#)

V Shoup - Manuscript, 2001 - [mirror.cr.yp.to](#)

... refer to a method of encrypting the message using such a shared random key as ... In particular, as the name implies, PSEC-KEM is a key encapsulation mechanism. ...

[Cited by 94](#) - [Related Articles](#) - [View as HTML](#) - [Web Search](#)

[PS] [A Proposal for an ISO Standard for Public Key Encryption \(Version 1.1\)](#) - [all 2 versions »](#)

V Shoup - ISO/IEC JTC 1/SC, 2001 - [shoup.net](#)

... 28 4.4 Changes from PSEC-2 ... There are traditional, and fairly well known "hybrid" schemes to do this: one first uses Diffie-Hellman to derive a shared key, and then ...

[Cited by 3](#) - [Related Articles](#) - [View as HTML](#) - [Web Search](#)

shared key distribution PSEC KEM

Search

[Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2008 Google

☒ Search only in Engineering, Computer Science, and Mathematics.

☐ Search in all subject areas.

Scholar All articles - [Recent articles](#) Results 1 - 10 of about 16,700 for [shared key distribution pub](#)

All Results

[U Maurer](#)

[M Bellare](#)

[S Bellare](#)

[R Canetti](#)

[D Denning](#)

[Timestamps in key distribution protocols](#)

DE Denning, GM Sacco - Communications of the ACM, 1981 - [portal.acm.org](#)

... acquire a shared communication key; in public-key systems [2], the users must acquire each others' public keys. Needham and Schroeder propose key distribution ...

[Cited by 464](#) - [Related Articles](#) - [Web Search](#)

[Secret key agreement by public discussion from common information - all 6 versions »](#)

UM Maurer - Information Theory, IEEE Transactions on, 1993 - [ieeexplore.ieee.org](#)

... Abstract-The problem of generating a shared secret key S ... but not sharing a secret key initially, is ... and Y according to some probability distribution P_{XYZ} , can ...

[Cited by 291](#) - [Related Articles](#) - [Web Search](#)

[An attack on the Needham-Schroeder public-key authentication protocol - all 15 versions »](#)

G Lowe - Information Processing Letters, 1995 - Elsevier

... that because the nonces are shared secrets, they ... GM Sacco, Timestamps in key distribution protocols, Comm. ... digital signatures and public-key cryptosystems, Comm ...

[Cited by 362](#) - [Related Articles](#) - [Web Search](#)

[Provably Secure Password-Authenticated Key Exchange Using Diffie-Heilman - all 12 versions »](#)

V Boyko, P MacKenzie, S Patel - Advances in Cryptology-Eurocrypt 2000, 2000 - [books.google.com](#)

... do not rely on any specific distribution of passwords ... we assume a password-authenticated

key exchange protocol ... authentication is performed using shared passwords ...

[Cited by 253](#) - [Related Articles](#) - [Web Search](#)

[Signcryption and Its Applications in Efficient Public Key Solutions - all 7 versions »](#)

Y Zheng - Information Security: First International Workshop, Isw'97, ..., 1998 - [books.google.com](#)

... key is derived from the Diffie-Hellman key $g^{x'xb} \bmod p$, or a key pre-distribution scheme [19]. ... In the case where a static key is a pre-shared random string ...

[Cited by 77](#) - [Related Articles](#) - [Web Search](#)

[New Public-Key Cryptosystem Using Braid Groups - all 12 versions »](#)

KH Ko, SJ Lee, JH Cheon, JW Han, J Kang, C Park, K ... - Advances in Cryptology-Crypto 2000: 20th Annual ..., 2000 - [books.google.com](#)

... ay 2^a . (d) B receives y , and computes the shared key $K =$ by ... 4. CH Bennet and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Proc. ...

[Cited by 131](#) - [Related Articles](#) - [Web Search](#)

[New multiparty authentication services and key agreement protocols - all 13 versions »](#)

G Ateniese, M Steiner, G Tsudik - Selected Areas in Communications, IEEE Journal on, 2000 - [ieeexplore.ieee.org](#)

... is very difficult in the centralized key distribution setting. ... sponding long-term public key of member obtains an (implicitly) authenticated shared key with ...

[Cited by 204](#) - [Related Articles](#) - [Web Search](#) - [Library Search](#)

[Encrypted key exchange: password-based protocols secure against dictionary attacks - all 84 versions »](#)

SM Bellovin, M Merritt - Research in Security and Privacy, 1992. Proceedings., 1992 ..., 1992 - [ieeexplore.ieee.org](#)

... Sec- tion 3 generalizes EKE, and shows how most public key distribution systems can be used. ... The password: a shared secret, often used as a key. ...

[Cited by 598](#) - [Related Articles](#) - [Web Search](#)

[Non-interactive public-key cryptography](#)

U Maurer, Y Yacobi - Advances in Cryptology—EUROCRYPT'91 (LNCS 547), 1991 - Springer
... of the preferred version of the proposed non-interactive public key distribution system follows. ... the mutual secure cipher key K_{AB} shared with user ...

[Cited by 88](#) - [Related Articles](#) - [Web Search](#)

[Provably secure session key distribution: the three party case - all 19 versions »](#)

M Bellare, P Rogaway - Proceedings of the twenty-seventh annual ACM symposium on ..., 1995 - [portal.acm.org](#)

... capture the idea of a "pure" key distribution. ... Many protocols aim to distribute a key whose value ... the identities of those who want to have the shared key. ...

[Cited by 305](#) - [Related Articles](#) - [Web Search](#)

Google ►

Result Page: 1 2 3 4 5 6 7 8 9 10 [Next](#)

[Google Home](#) - [About Google](#) - [About Google Scholar](#)